

# VIPNet QKDSim – от простого к сложному



техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

Иванов Олег  
Менеджер

# ViPNet QKDSim



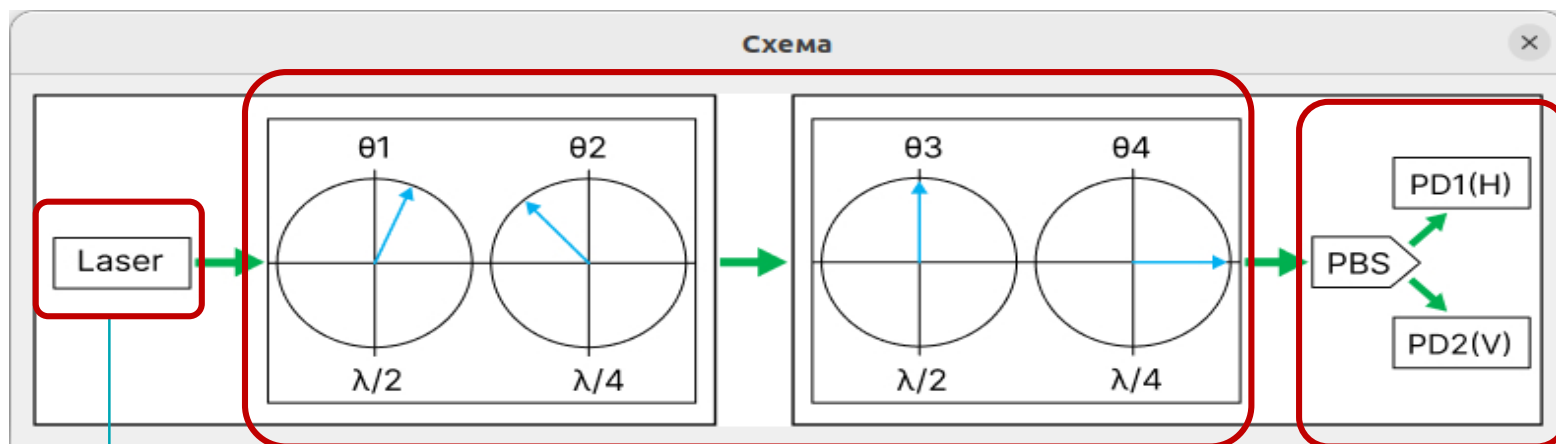
ViPNet QKDSim наглядно показывает эмуляцию принципов квантового распределения ключей, основанного на принципах генерации и считывания оптических информационных состояний.

Информация в оптических состояниях кодируется и декодируется путем изменения параметров поляризации генерируемого светового потока, которые интерпретируются как параметры протоколов КРК.

# Назначение ViPNet QKDSim

- Подготовка специалистов по информационной безопасности
- Подготовка специалистов по квантовым технологиям
- Обучение в продвинутых школах и колледжах

# Оптическая схема

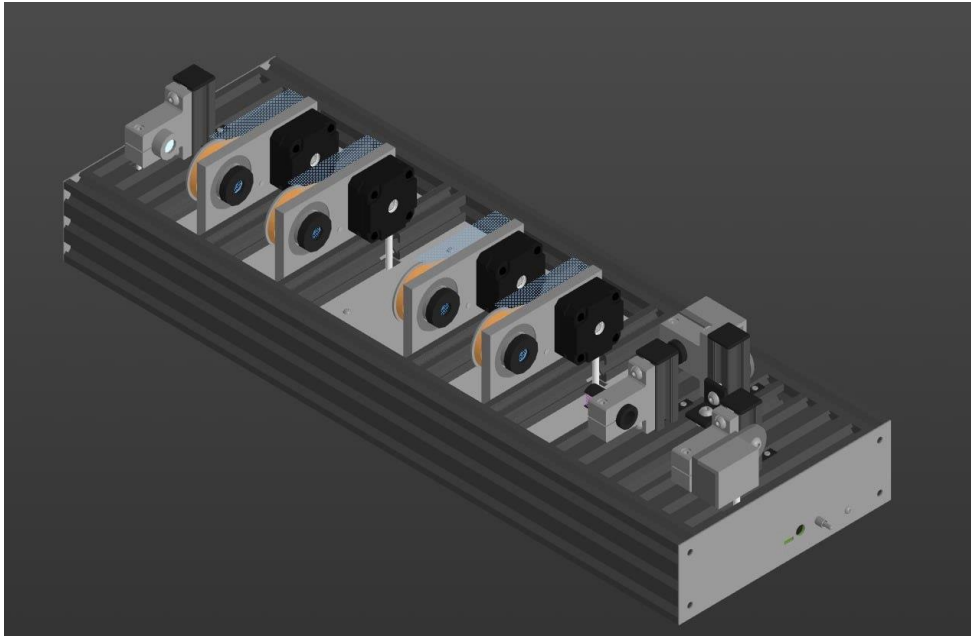


Алиса  
Лазер

Модулятор  
поляризации света

Боб  
Поляризационный куб и  
2 фотодетектора

# Аппаратная платформа



## Особенности:

- Управление с помощью ПК (ноутбука)
- Усиливает восприятие материала
- Возможность установить дополнительные элементы

# Применение в образовательной сфере

## Физические основы

Формирование поляризационных состояний

Регистрация поляризованного света

## Классическая передача информационных бит

Принципы поляризационного кодирования бит

Принципы детектирования бит

Шумы в детекторах

Ошибки передачи

## Квантовая передача информационных бит

Детектирование одиночных фотонов

Шумы в детекторах

Ошибки передачи

## Квантовое распределение ключей

Понятие о базисах кодирования

Алгоритмы формирования и детектирования посылок

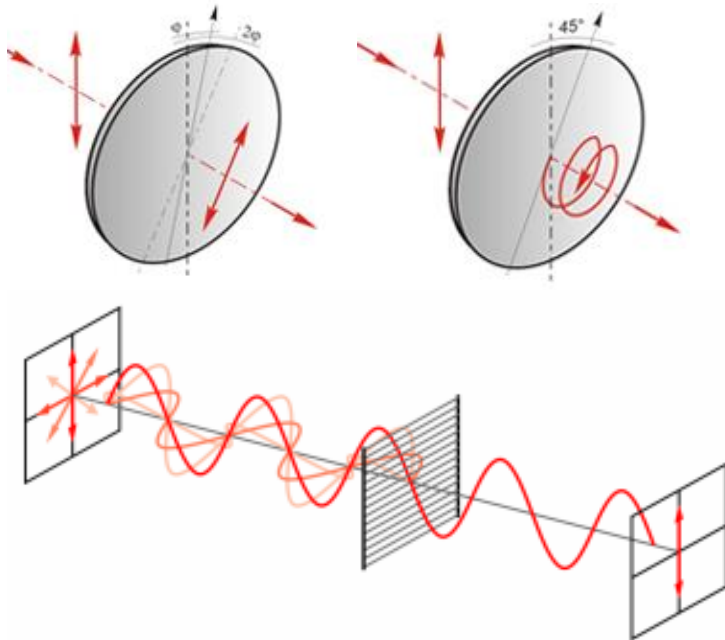
Постобработка распределяемой последовательности

## Безопасность передачи и распределения ключей

Проведение атак на протоколы и системы КРК

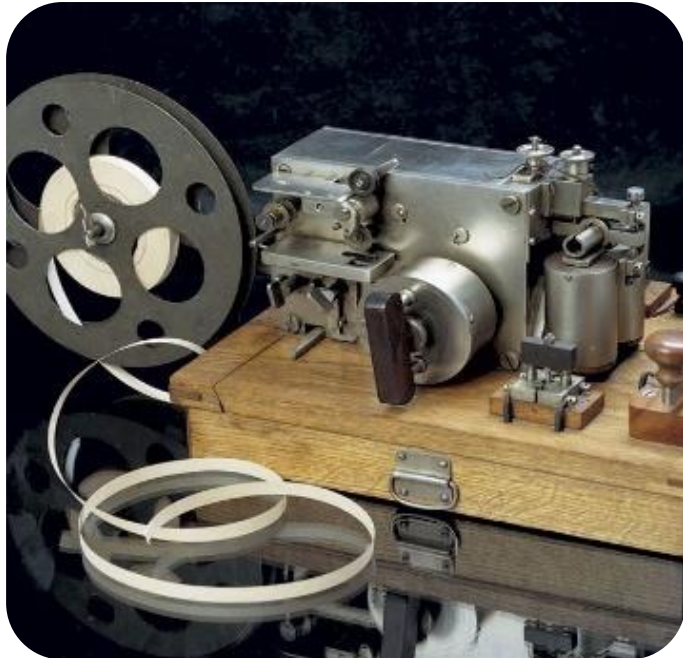
Связь ошибки распределения ключей с информацией, доступной нарушителю

# Изучение физических основ: темы



- Поляризация света
- Волновые пластины
- Управление поляризацией света (модуляция/демодуляция)
- Поляризатор-анализатор и регистрация света
- Базисы измерений

# Распределение ключей (информационных бит): темы

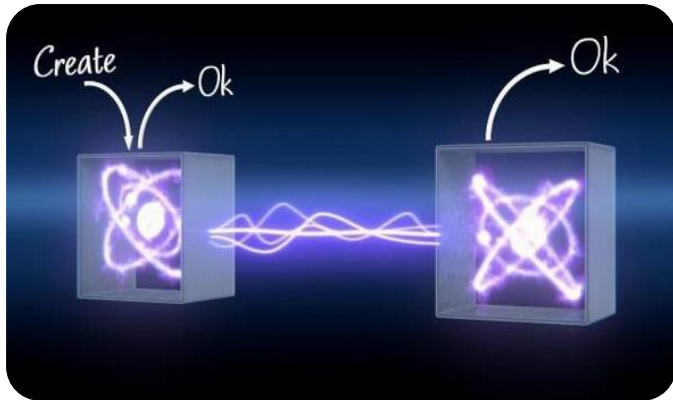


## Классические системы приёма-передачи

- Классическая передача информации
- Распределение информации с классическим излучателем
- Влияние чувствительности и шумов детекторов на классическую передачу информации (устойчивость системы)
- Влияние нарушителя на классическую передачу информации



# Распределение ключей (информационных бит): темы

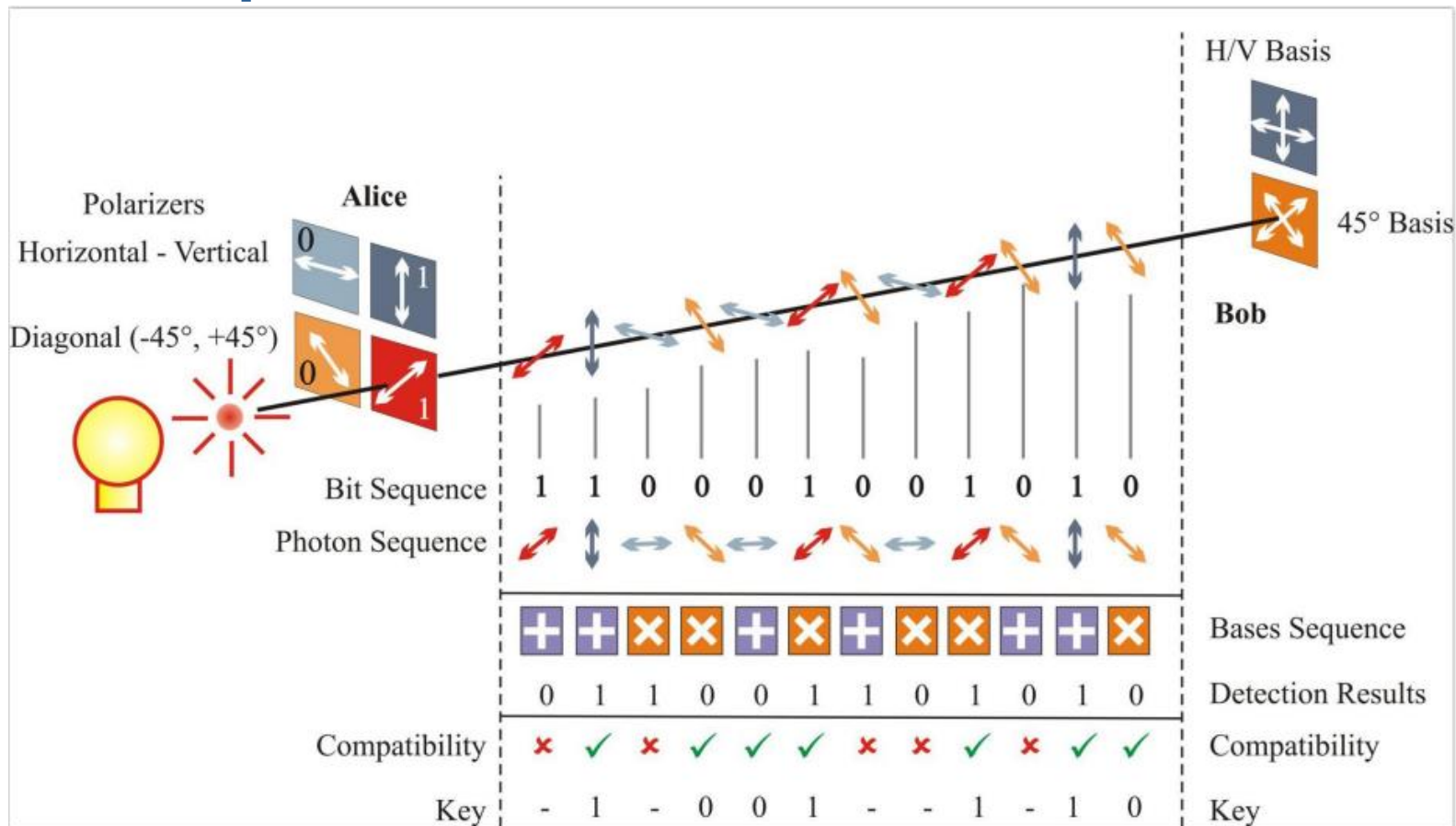


## Квантовые системы приёма-передачи

- Однофотонные и квазиоднофотонные излучатели
- Квантовое распределение ключей (информационных бит)
- Влияние чувствительности и шумов детекторов на квантовое распределение ключей (устойчивость системы)
- Влияние нарушителя на квантовое распределение ключей (информационных бит)

# Протокол ВВ84

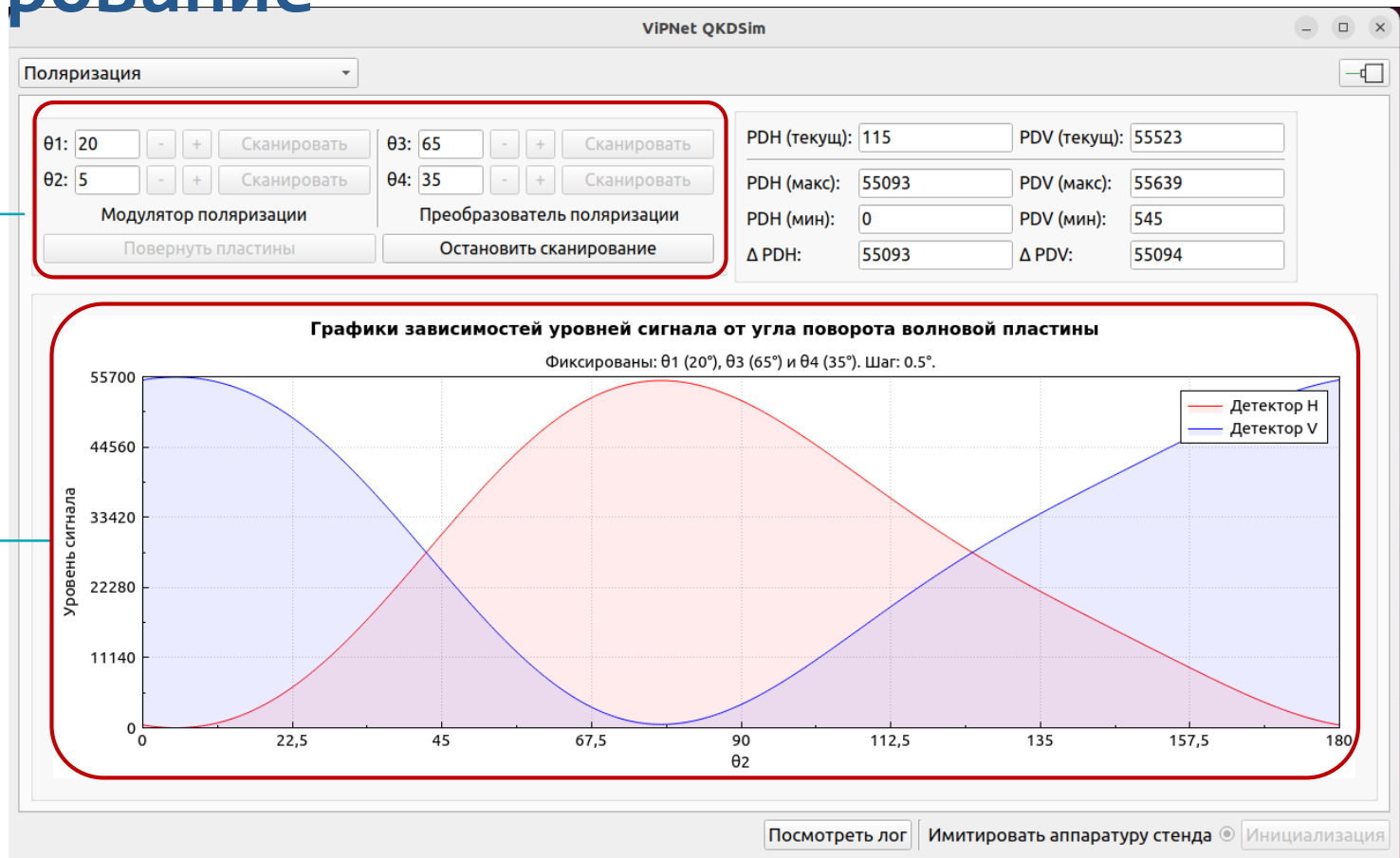
# Схема протокола BB84



# Определение базиса и сканирование

Задаем значения углов поворота пластин и запускаем сканирование пластины  $\theta_2$

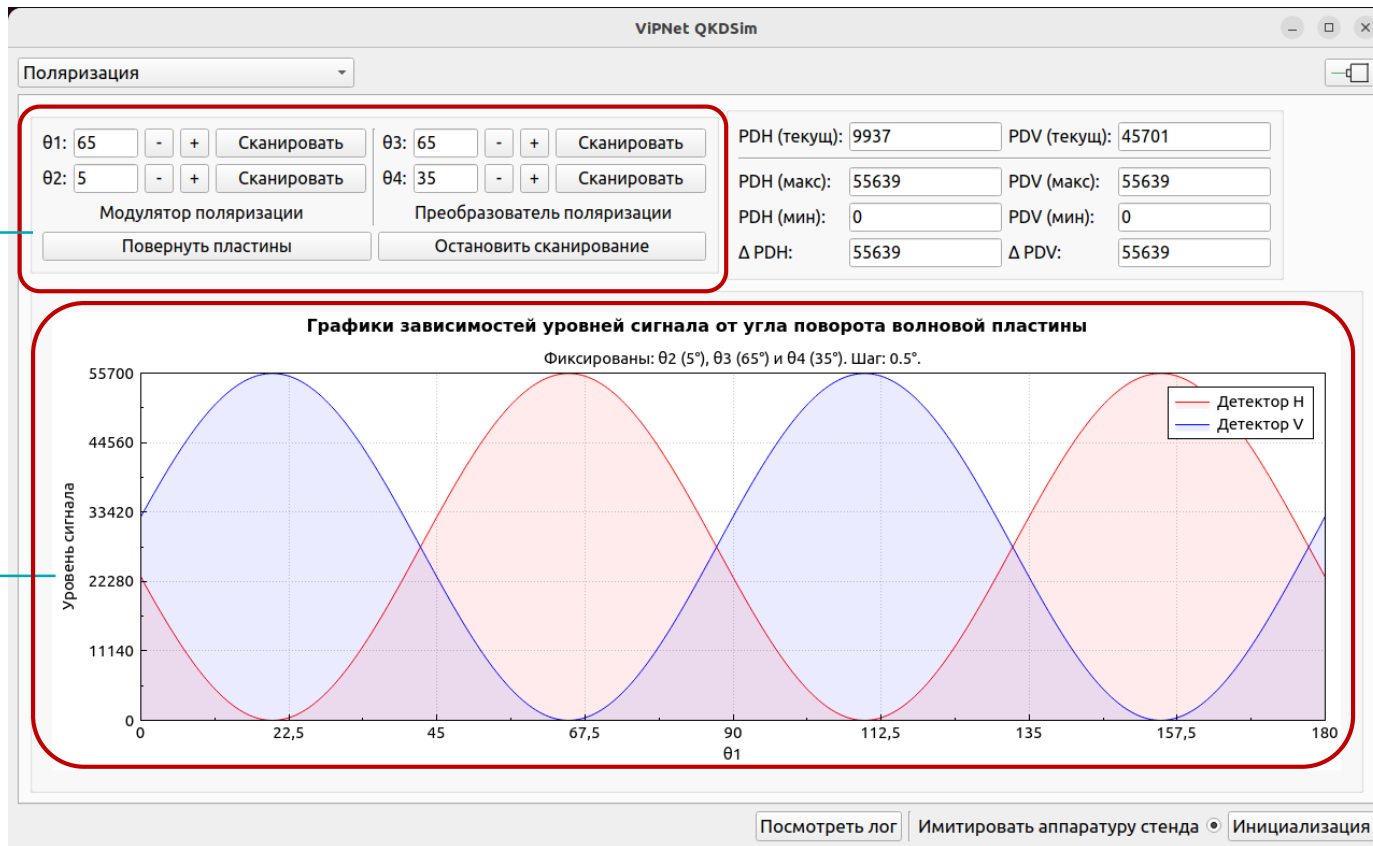
Полученный график



# Определение базиса и сканирование

Задаем значения углов поворота пластин и запускаем сканирование пластины  $\theta_1$

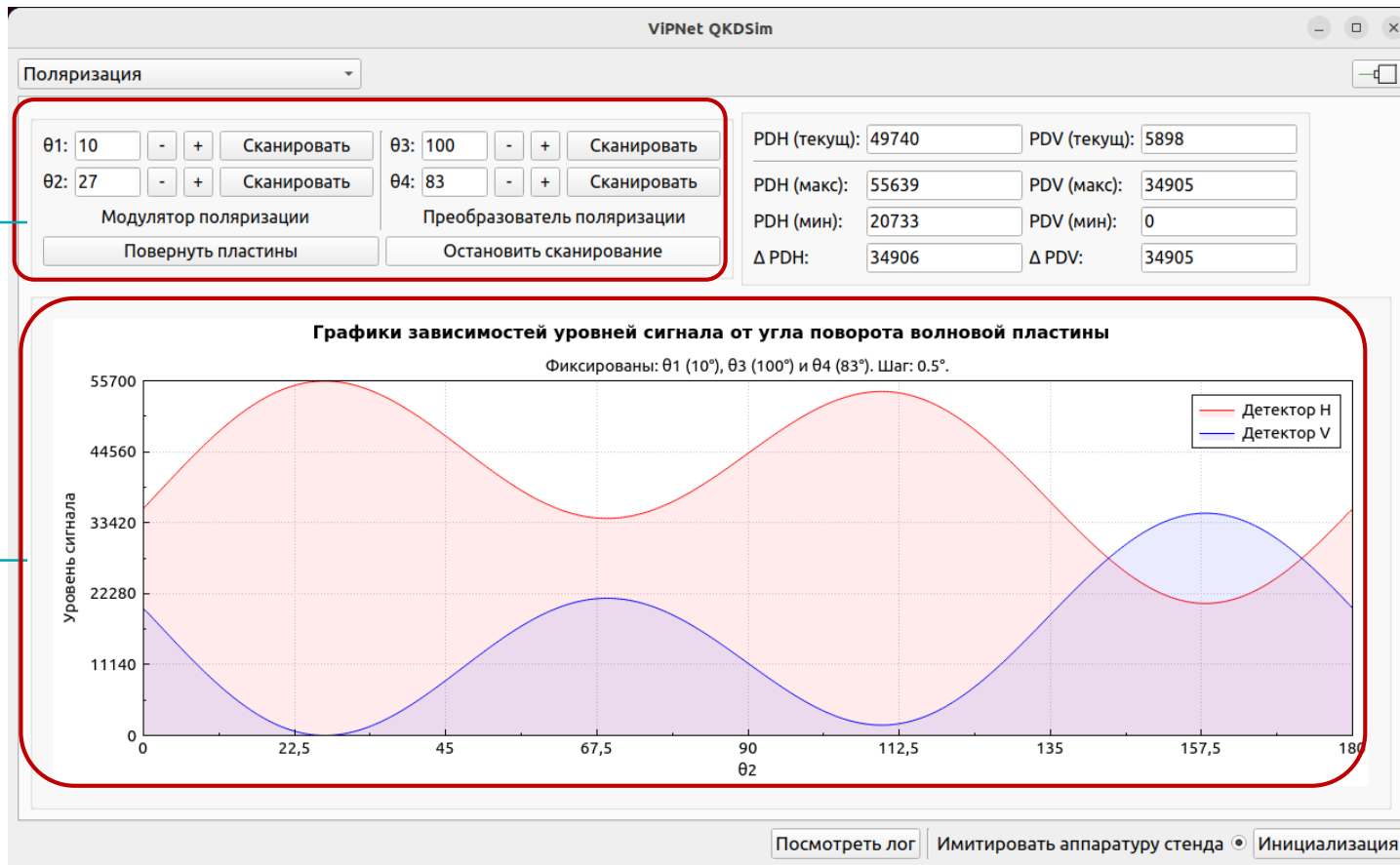
Полученный график



# Подбор конфигурации углов

Задаем значения углов поворота пластин и запускаем сканирование пластины  $\theta_2$

Полученный график



# Настройка правил протокола


Настройка правил протокола

Добавить базис    Загрузить правила    Сохранить правила

Активно	Базис	Бит	$\theta 1$	$\theta 2$	$\theta 3$	$\theta 4$	PH	PV
<input checked="" type="checkbox"/>	0	0	20	5	65	35	1	0
		1	65	5	65	35	1	0
<input checked="" type="checkbox"/>	1	0	10	27	100	83	0	1
		1	55	27	100	83	0	1

Результаты сканирования углов добавляем в настройки правил протокола

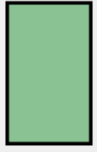
# Имитируемые параметры



**Источник излучения**


Классический  
 Однофотонный  
 Квазиоднофотонный

μ:



**Атаки**

Выключены  
 Ослепление  
 MiTM



**Параметры детекторов**

	PD1	PD2
Шум/сиг.:	0	0
Чувст-ть:	1	1

Изменений нет. Применить

Имитация источника излучения

Имитация нарушителя

Имитация параметров детекторов



# Тестовая комбинация

VIPNet QKDSim

Протоколы Имитируемые параметры Правила

Алиса (выбор базиса):	0000111100001111	16	Авто	Старт
Алиса (выбор бита):	0011001100110011	16	Авто	Сброс
Боб (выбор базиса):	0000111111110000	16	Авто	Шаг
Боб (выбор бита):	0101010101010101	16	Авто	

Сырая строка	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1
Сравнение базисов	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1
Проверка ошибок	0	0	1	1	0	0	1	1							
Чистая строка	0	0	1	1	0	0	1	1							

Длина ключа: 8 Доля нулей: 0.5  
Bit error: 0% Доля единиц: 0.5  
Ключ: 00110011  
Биты Евы: \_\_\_\_\_

Посмотреть лог Имитировать аппаратуру стенда Инициализация

Тестовая комбинация кодируемых базисов и бит

Результаты выполнения протокола

# Тестовая комбинация

VIPNet QKDSim

Протоколы:  Имитируемые параметры: Правила

Алиса (выбор базиса): 1111111101100011110110001101010011000010101000111101011011100000101111010011000011011110011010001000100010101000001010100011001101110 500

Алиса (выбор бита): 0110011010100001110010111000010110001110110110010111010100011110101001101011110010001111101101100111100001001101101101101001011 500

Боб (выбор базиса): 0010111000101110010011010100100001111010001010110010100010111101100001011001110110000001101001010001010001000000000101000 500

Боб (выбор бита): 01010100110101101100111010011101101010000010100000001110001111001110010000100111010110001001011110010011111010100011011011110001 500

Шаг	Алиса (базис)	Алиса (бит)	Боб (базис)	Боб (бит)
1	0	1	0	1
2	0	1	0	1
3	1	0	0	0
4	1	0	0	0
5	1	0	0	0
6	1	0	0	0
7	1	0	0	0
8	1	0	0	0
9	1	0	0	0
10	1	0	0	0
11	1	0	0	0
12	1	0	0	0
13	1	0	0	0
14	1	0	0	0
15	1	0	0	0
16	1	0	0	0
17	1	0	0	0
18	1	0	0	0
19	1	0	0	0
20	1	0	0	0
21	1	0	0	0
22	1	0	0	0
23	1	0	0	0
24	1	0	0	0
25	1	0	0	0
26	1	0	0	0
27	1	0	0	0
28	1	0	0	0
29	1	0	0	0
30	1	0	0	0
31	1	0	0	0
32	1	0	0	0

Сырая строка	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	1	1	1	0	1	0	1	1	1	0	0	0	0	0	1
Сравнение базисов	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	1	0	0	0	0	1
Проверка ошибок	0	1	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
Чистая строка	0	1	1	1	0	0	0	0	1	0	0	1	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	

Длина ключа: 265 Доля нулей: 0.524528

Bit error: 0% Доля единиц: 0.475472

Ключ: 0110110100111000011110111100100101100011

Биты Евы:

Увеличим количество бит до 500

Результаты выполнения протокола



# Спасибо за внимание!

Иванов Олег  
Oleg.Ivanov@infotecs.ru

---

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)